

Claims:

Claims

5 We claim:

1. A method of transmitting a data payload from a sender station to a recipient station comprising:

- 10 (a) assigning a sender ID key to one or more stations belonging to a sender;
- (b) assigning a recipient ID key to one or more stations belonging to a recipient;
- (c) assigning a server public key to a server;
- 15 (d) assigning a server private key to the server, wherein the server private key and the server public key are a complementary pair of keys;
- (e) at the sender station:
 - (i) generating a session key;
 - 20 (ii) encrypting the session key with the server public key to produce a first sender encrypted session key;
 - (iii) encrypting the session key with the sender ID key to produce a second sender encrypted session key;
 - (iv) encrypting the data payload and the second encrypted session key with the session key to produce a sender
25 encrypted payload;
 - (v) transmitting the sender encrypted payload and the first sender encrypted session key to the server;
- (f) at the server:
 - 30 (i) decrypting the first sender encrypted session key with the server private key to obtain a first server decrypted session key;

- 58 -

- 5
- (ii) decrypting the sender encrypted payload with the first server decrypted session key to obtain the payload and the second sender encrypted session key;
- (iii) determining the sender associated with the payload based on information transmitted from sender;
- (iv) decrypting the second sender encrypted session key with the sender ID key to obtain a second server decrypted session key;
- 10 (v) comparing the first server decrypted session key to the second server decrypted session key;
- (vi) if the result of the comparison is that the first and second server decrypted session keys are identical, then accepting the transmission as having originated from the sender station.
- 15

2. The method of claim 1 wherein, if the result of the comparison in (f)(v) is that the first and second server decrypted session keys are identical, then:

- (g) at the server:
- 20 (i) encrypting the session key with the recipient ID key to produce a first server encrypted session key;
- (ii) encrypting the session key with the server private key to produce a second server encrypted session key;
- (iii) encrypting the data payload and the second server encrypted session key with the session key to produce a server encrypted payload; and
- 25 (iv) transmitting the first server encrypted session key and the server encrypted payload to the recipient station; and
- (h) at the recipient station:
- 30 (i) decrypting the first server encrypted session key with the recipient ID key to produce a first recipient decrypted session key;

- 59 -

- 5
- (ii) decrypting the server encrypted payload with the session key to obtain the data payload and the second server encrypted session key;
 - (iii) decrypting the second server encrypted session key with the server public key to produce a second recipient decrypted session key; and
 - (iv) comparing the first recipient decrypted session key with the second recipient decrypted session key; and
 - 10 (v) if the result of the comparison is that the first and second recipient decrypted session keys are identical, then accepting the data payload as having been sent from the server.

3. The method of claim 2 wherein the first sender encrypted session key
15 and the sender encrypted payload may be compressed before transmission.

4. The method of claim 3 wherein the compressed first sender encrypted session key and the sender encrypted payload are decompressed upon receipt at the server.

20

5. The method of claim 2 wherein the first server encrypted session key and the server encrypted payload may be compressed before transmission.

6. The method of claim 5 wherein the compressed first server encrypted session key and the server encrypted payload are decompressed upon receipt at the recipient.

7. The method of claim 1, wherein, if the result of the comparison in (f)(v) is that the first and second server decrypted session keys are identical, then
30 sending a confirmation message from the server to the sender station.

- 60 -

8. The method of claim 2, wherein, if the result of the comparison in (h)(iv) is that the first and second server decrypted session keys are identical, then sending a confirmation message from the recipient station to the server.
- 5 9. The method of claim 8, wherein a confirmation message is sent from the server to the sender station, upon receipt of a confirmation message at the server sent by the recipient station.
- 10 10. The method of claim 1, comprising storing a hash of the payload upon the server.
11. The method of claim 1 wherein, if the result of the comparison in (f)(v) is that the first and second server decrypted session keys are identical, then:
- (g) at the server:
- 15 (i) generating a session key;
- (ii) encrypting the server generated session key with the recipient ID key to produce a first server generated encrypted session key;
- (iii) encrypting the server generated session key with the
- 20 server private key to produce a second server generated encrypted session key;
- (iv) encrypting the data payload and the second server generated encrypted session key with the server generated session key to produce a server encrypted
- 25 payload; and
- (v) transmitting the first server generated encrypted session key and the server encrypted payload to the recipient station; and
- (h) at the recipient station:
- 30 (i) decrypting the first server generated encrypted session key with the recipient ID key to produce a first recipient decrypted server generated session key;

- 61 -

- 5
- (ii) decrypting the server encrypted payload with the server generated session key to obtain the data payload and the second server generated encrypted session key;
 - (iii) decrypting the second server generated encrypted session key with the server public key to produce a second recipient decrypted server generated session key; and
 - (iv) comparing the first recipient decrypted server generated session key with the second recipient server generated decrypted session key; and
 - (v) if the result of the comparison is that the first and second recipient server generated decrypted session keys are identical, then accepting the data payload as having been sent from the server.
- 10
- 15

12. The method of claim 11 wherein the first sender encrypted session key and the sender encrypted payload may be compressed before transmission.

13. The method of claim 12 wherein the compressed first sender encrypted session key and the sender encrypted payload are decompressed upon receipt at the server.

20

14. The method of claim 11 wherein the first server generated encrypted session key and the server encrypted payload may be compressed before transmission.

25

15. The method of claim 14 wherein the compressed first server generated encrypted session key and the server encrypted payload are decompressed upon receipt at the recipient.

30

16. The method of claim 11 wherein, if the result of the comparison in (h)(iv) is that the first recipient decrypted server generated session key and

- 62 -

the second recipient server generated decrypted session key are identical, then sending a confirmation message from the recipient station to the server.

17. The method of claim 16, wherein upon receipt at the server of a confirmation message from the recipient station to the server, a confirmation message is sent to the sender station.

18. A method of transmitting documents from a sender station to a recipient station comprising:

- 10 (a) creating a document at a sender station and specifying recipient information upon said document;
- (b) creating files representative of said document;
- (c) identifying said recipient information upon said document;
- 15 (d) transmitting said representative files and said recipient information to a server.
- (e) receiving said representative files and said recipient information at said server;
- (f) determining at said server an electronic address associated with said recipient information; and
- 20 (g) transmitting from said server to a recipient said representative files via said electronic address.

19. The method of claim 18 including invoking a software application and wherein steps (b), (c) and (d) are performed by the software application.

20. The method of claim 18 where said representative files may be machine and/or human readable files.

21. The method of claim 18 wherein said electronic transmission means may be an e-mail address.

- 63 -

22. The method of claim 18 wherein said electronic transmission means may be an FTP address.

23. The method of claim 18 wherein said electronic transmission means
5 may be associated with protocols based on TCP-IP.

24. A method of transmitting documents from a sender to a recipient comprising:

- 10 (a) creating a document at a sender station and specifying recipient information upon said document;
- (b) creating a machine readable version of the document, wherein the machine readable version identifies the recipient based on the recipient information; and
- 15 (c) transmitting said machine readable version of the document, wherein said server receives said recipient information and said machine readable version and determines an electronic address associated with said recipient, and transmits said representative files to said recipient via said electronic transmission means.

20

25. The method of claim 24 further including creating a human readable file corresponding to the document and transmitting the human readable file with the machine-readable file.

25 26. The method of claim 24 wherein said electronic transmission means may be an e-mail address.

27. The method of claim 24 wherein said electronic transmission means may be an FTP address.

30

28. The method of claim 24 wherein said electronic transmission means may be associated with a TCP-IP address or transmission protocol.

- 64 -

29. A method for creating a document map for a document, wherein the document is of a document type, the method comprising:
- (a) defining a document schema, wherein the document schema contains attributes associated the document type
 - 5 (b) mapping different regions of the document and correlating each mapped region to an attribute.
30. The method of claim 29 wherein one or more of the attributes may be assigned a default value.
31. The method of claim 29 wherein a mapped region on said document is
10 defined by a relative position of an attribute.
32. A method of parsing a document to create a machine readable version of the document, the method comprising:
- (a) receiving the document in an electronic form;
 - 15 (b) extracting text elements of the document and recording the coordinates of each text element;
 - (c) comparing the coordinates of each extracted text element with regions defined in a document map; and
 - (d) identifying an attribute for each extracted text element based on the comparison; and
 - 20 (e) recording each extracted text element according to its attribute in the machine readable file.
33. The method of claim 32 further comprising tagging each extracted text element according to its attribute and identifying each tagged extracted text
25 elements together by its tag in the machine readable file.
34. The method of claim 32, wherein the tags are XML tags.

- 65 -

35. The method of claim 32, wherein the attributes in the machine-readable file may be associated with a default value.

36. A method of configuring a sender station, a server, and a recipient
5 station with keys to be used to encrypt data comprising:

(a) assigning a server public key to the server;

(b) assigning a server private key to the server; wherein the server private key and the server public key are a complimentary pair of keys;

10 (c) distributing the server public key to the sender and recipient stations;

(d) generating at the sender station a sender ID key and transmitting the sender ID key to the server, wherein it is stored securely; and

15 (e) generating at the recipient station a recipient ID key and transmitting the recipient ID key to the server, wherein it is stored securely.

37. A method of transmitting a data payload from a sender station to a recipient station comprising:

(a) assigning a server public key to a server;

20 (b) assigning a server private key to the server; wherein the server private key and the server public key are a complimentary pair of keys;

(c) distributing the server public key to the sender and recipient stations;

25 (d) generating at the sender station a sender ID key and transmitting the sender ID key to the server, wherein it is stored securely;

- 66 -

(e) generating at the recipient station a recipient ID key and transmitting the recipient ID key to the server, wherein it is stored securely;

5 (f) at the sender station:

- (i) generating a session key;
- (ii) encrypting the session key with the server public key to produce a first sender encrypted session key;
- (iii) encrypting the session key with the sender ID key to produce a second sender encrypted session key;
- 10 (iv) encrypting the data payload and the second encrypted session key with the session key to produce a sender encrypted payload;
- (v) transmitting the sender encrypted payload and the first sender encrypted session key to the server;

15

(g) at the server:

- (i) decrypting the first sender encrypted session key with the server private key to obtain a first server decrypted session key;
- 20 (ii) decrypting the sender encrypted payload with the first server decrypted session key to obtain the payload and the second sender encrypted session key;
- (iii) determining the sender associated with the payload based on information transmitted from sender;
- 25 (iv) decrypting the second sender encrypted session key with the sender ID key to obtain a second server decrypted session key;
- (v) comparing the first server decrypted session key to the second server decrypted session key;
- 30 (vi) if the result of the comparison is that the first and second server decrypted session keys are identical, then

- 67 -

accepting the transmission as having originated from the sender station.

38. The method of claim 37 wherein, if the result of the comparison in
5 (g)(v) is that the first and second server decrypted session keys are identical, then:

- (h) at the server:
 - (i) encrypting the session key with the recipient ID key to produce a first server encrypted session key;
 - 10 (ii) encrypting the session key with the server private key to produce a second server encrypted session key;
 - (iii) encrypting the data payload and the second server encrypted session key with the session key to produce a server encrypted payload; and
 - 15 (iv) transmitting the first server encrypted session key and the server encrypted payload to the recipient station; and
- (i) at the recipient station:
 - (i) decrypting the first server encrypted session key with the recipient ID key to produce a first recipient decrypted session key;
 - 20 (ii) decrypting the server encrypted payload with the session key to obtain the data payload and the second server encrypted session key;
 - (iii) decrypting the second server encrypted session key with the server public key to produce a second recipient decrypted session key; and
 - 25 (iv) comparing the first recipient decrypted session key with the second recipient decrypted session key; and
 - (v) if the result of the comparison is that the first and second recipient decrypted session keys are identical, then
 - 30

- 68 -

accepting the data payload as having been sent from the server.

39. The method of claim 37 wherein, if the result of the comparison in
5 (g)(v) is that the first and second server decrypted session keys are identical, then:

- (h) at the server:
 - (i) generating a session key;
 - (ii) encrypting the server generated session key with the
10 recipient ID key to produce a first server generated encrypted session key;
 - (iii) encrypting the server generated session key with the server private key to produce a second server generated encrypted session key;
 - (iv) encrypting the data payload and the second server
15 generated encrypted session key with the server generated session key to produce a server encrypted payload; and
 - (v) transmitting the first server generated encrypted session
20 key and the server encrypted payload to the recipient station; and
- (i) at the recipient station:
 - (i) decrypting the first server generated encrypted session
25 key with the recipient ID key to produce a first recipient decrypted server generated session key;
 - (ii) decrypting the server encrypted payload with the server generated session key to obtain the data payload and the second server generated encrypted session key;
 - (iii) decrypting the second server generated encrypted
30 session key with the server public key to produce a

- 69 -

second recipient decrypted server generated session key;
and

- 5 (iv) comparing the first recipient decrypted server generated session key with the second recipient server generated decrypted session key; and
- (v) if the result of the comparison is that the first and second recipient server generated decrypted session keys are identical, then accepting the data payload as having been sent from the server.

10 40. The method of claim 36 wherein the sender ID key may be associated with one or more stations belonging to a sender.

41. The method of claim 36 wherein the recipient ID key may be associated with one or more stations associated with a sender.

15